Trustwave®

DATA SHEET

Trustwave DbProtect

ENTERPRISE DATA SECURITY PLATFORM

Benefits

- Leverage a highly scalable solution that gives you real-time visibility and protection for your databases against advanced, persistent, stealthy and insider threats
- Gain end-to-end visibility and protection for critical databases across your entire organization – both on-premise and in the cloud.
- Get a unified view and quick access to database assets, vulnerabilities, risk levels, user privileges, anomalies and incidents in real time with a single dashboard.
- Detect, alert and take corrective action against suspicious activities, intrusions and policy violations in real time
- Demonstrate compliance with more than one set of business, security, or regulatory policies with powerful reporting features that are easily customized to meet specific business needs.

A database is often called the backbone of an organization. Databases contain sensitive and proprietary information - such as employee information, medical records, customer information, financial data and more – making them a prized target for cyber criminals who constantly look for ways to access valuable data for large financial payoffs. Simply securing the perimeter is no longer enough - businesses need to protect their databases on top of securing their networks and applications. As databases become more challenging to secure, organizations are also finding it difficult to find and retain resources to implement effective database security controls.

DbProtect is a highly scalable data security platform that enables organizations to secure their relational databases and big data stores, both on premise and in the cloud, with a distributed architecture and enterprise level analytics. DbProtect empowers organizations to uncover database configuration errors, identify access control issues, missing patches, and toxic combination of settings that could lead to escalation of privileges attacks, data leakage, denial-of-service (DoS), or unauthorized modification of data held within data stores across their environments.

Highly scalable, Enterprise Class Database Security Platform

Secure relational databases and big data stores across your environment, both on premise and in the cloud, with multi-user/role-based access, a distributed architecture, and enterprise-level analytics, Trustwave DbProtect enables large organizations to meet their scalability requirements across thousands of data stores.

Complete, Accurate and Intuitive Data Security Solution

Automated inventory testing, information gathering, and analysis give you the information you need to harden the security of your data stores.

Manage Data Security Assessment Results and Remediation Efforts

Facilitate closing the loop from initial discovery of relational databases and big data stores to fixing vulnerabilities and policy violations.

Monitor Database Activity for Security Violations

Identify and alert on unusual or suspicious behavior to help correlate with other network events.

Continuously Updated Data Security Knowledgebase

Extensive and continuously updated analytics and knowledgebase of relational database and big data security best practices, configuration settings, and vulnerabilities backed by Trustwave SpiderLabs.

Features

Database Discovery and Inventory

- Easily identify databases across your entire enterprise along with their respective objects, users and enabled security features within your organization.
- Easily discover and review all the accessible assets, user access levels, and security feature usage throughout your environment.
- Identify and highlight recently added, rogue or missing data store installations and objects.

Conduct Vulnerability and Configuration Assessments

- Demonstrate effective controls for sensitive data and compliance with more than one set of business, security, or regulatory policies as well as IT audits.
- Examine data stores for vulnerability, configuration, and user rights issues with built-in and customized policies.

Identify Excessively Privileged User Accounts

- Proactively establish an environment of least privilege by gaining visibility into who has access to your sensitive data by identifying users, roles and privileges.
- Establish meaningful controls that track how users interact with the data and capture an audit trails by identifying who has access to what data and why/how they've been granted that access.

Implement Risk Mitigation and Compensating Controls

- Reduce your risk of compromise and narrow the scope of required compensating controls by remediating high-risk vulnerabilities and misconfigurations within your database.
- Assign exceptions for vulnerabilities that cannot get remediated or patched in a timely manner
- Using data analytics to associate risk scores with the results/findings of your vulnerability assessment to identify your most exposed systems or groups. You can then focus your efforts where you stand to make the most impact.

Audit Privileged User Behavior in Real Time

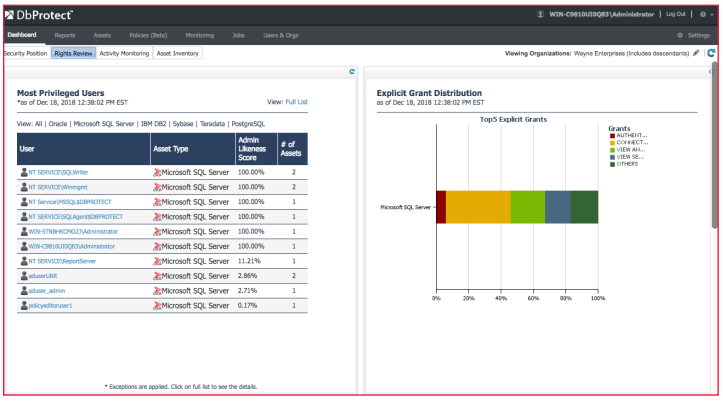
- Collect a forensic audit trail of all privileged activities in a database to meet compliance regulations (including Sarbanes-Oxley) that require tracking of structural changes in your information, which means auditing privileged (administrative) activity, not just the actions of known privileged users.

Detect, alert and respond to policy violations in real time

- Send alert messages in syslog, snmp, or flat file for operations center personnel to take appropriate action when a security violation is identified.
- Depending on the policy violation and the sensitivity of the affected system or data, automated and scripted responses can contain the threat and give the security team time to investigate and take corrective action.

Reporting, Integration and Analytics

- With a consolidated view of vulnerabilities, threats, risks, and compliance efforts across heterogeneous data store environments you gain the ability run analytics and report against your current status, demonstrate progress, effectiveness, and operational efficiency
- Evaluate trends and drill down for detailed views of each individual database, group of databases, or databases of specific business units or groups within the enterprise.



WHY TRUSTWAVE DBPROTECT?

Trustwave DbProtect is a complete database security platform that automates the securing of critical data where it's stored with database vulnerability management, database user rights management and database activity monitoring (DAM).

Trustwave DbProtect inventories and classifies databases and discovers vulnerabilities, configuration mistakes, access control issues, missing patches or any toxic combination thereof in popular databases. Trustwave DbProtect gives a detailed picture of database user accounts, data ownership, access controls and rights to sensitive information to restrict user privileges to the minimum necessary. Trustwave DbProtect also monitors for deviations in database traffic to detect suspicious activity and provide real-time warnings and build an audit trail.

Trustwave®

For more information: www.trustwave.com